We claim:

1. A system for securely providing biometric input from a user, comprising:

a biometric sensor;

a security component which provides security functions, such that the security component can vouch for authenticity of components with which it is securely operably connected;

a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

a card reader for accessing the stored secrets and stored identifying information;

means for operably inserting the card into the card reader; and

means for securely operably connecting the biometric sensor, the card reader, and the security component.

2. The system according to Claim 1, wherein the stored identifying information comprises stored biometric information of the authorized holder, and further comprising means for comparing biometric information obtained with the biometric sensor from a user of the system, to the stored biometric information of the authorized holder.

3. The system according to Claim 1, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

4. The system according to Claim 1, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

5. The system according to Claim 4, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

6. The system according to Claim 1, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

7. The system according to Claim 1, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

8. The system according to Claim 1, wherein the means for securely operably connecting further comprises means for authenticating the biometric sensor and the card reader to the security component.

9. The system according to Claim 8, further comprising means for authenticating the security component to the biometric sensor and the card reader.

10. The system according to Claim 1, wherein the means for securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

11. The system according to Claim 8, wherein the means for authenticating the biometric sensor and the card reader are securely stored thereon.

12. The system according to Claim 8, wherein the means for authenticating further comprises means for using public key cryptography.

13. The system according to Claim 2, further comprising means for concluding that the user is the authorized holder of the card only if the means for comparing succeeds.

14. The system according to Claim 1, wherein the card is a smart card.

15. The system according to Claim 2, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising means for digitally signing information presented to the card with the private key if the means for comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

16. The system according to Claim 2, wherein the means for comparing is performed by the biometric sensor.

17. The system according to Claim 16, further comprising means for securely transferring the stored biometric information of the authorized holder to the biometric sensor for use by the means for comparing.

18. The system according to Claim 17, further comprising means for interrupting the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

19. The system according to Claim 2, wherein the means for comparing is performed by the security component.

20. The system according to Claim 15, further comprising means for securely operably connecting an application processing component to the security component, and wherein the information presented to the card is generated by the securely operably connected application processing component.

21. The system according to Claim 8, wherein the means for authenticating further comprises means for performing a security handshake between the biometric sensor and the security component and between the card reader and the security component.

22. The system according to Claim 21, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

23. The system according to Claim 8, wherein:

the means for authenticating the biometric sensor further comprises means for using (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

the means for authenticating the card reader further comprises means for using (1) a second unique identifier of the card reader, (2) a second digital signature computed over the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.

24. A card which contains one or more previously-stored secrets of an authorized holder of the card and which has a biometric sensor embedded on a surface thereof.

25. The card according to Claim 24, wherein the biometric sensor is a fingerprint sensor, and wherein the previously-stored secrets include a fingerprint of the authorized card holder.

26. The card according to Claim 24, wherein the biometric sensor is a palm print sensor, and wherein the previously-stored secrets include a palm print of the authorized card holder.

27. The card according to Claim 24, wherein the biometric sensor is a voice print sensor, and wherein the previously-stored secrets include a voice print of the authorized card holder.

28. The card according to Claim 24, wherein the biometric sensor is a retina scanner, and wherein the previously-stored secrets include a retina scan of the authorized card holder.

29. The card according to Claim 24, wherein the biometric sensor is a skin chemistry sensor, and wherein the previously-stored secrets include a skin chemistry of the authorized card holder.

30. The card according to Claim 24, wherein the previously-stored secrets include stored biometric information of the authorized holder, and further comprising means for comparing biometric information that is obtained with the biometric sensor from a user, to the stored biometric information of the authorized holder.

31. The card according to Claim 30, further comprising means for accessing selected ones of the previously-stored secrets only if the means for comparing determines that the obtained biometric information of the user matches the stored biometric information of the authorized holder.

32. The card according to Claim 31, wherein the previously-stored secrets include a private cryptographic key of the authorized holder, and wherein the means for accessing further comprising means for accessing the private key to compute a digital signature over information presented to the card.

33. A computer program product for securely providing biometric input from a user, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for operating a biometric sensor;

computer-readable program code means for operating a security component which provides security functions, such that the security component can vouch for authenticity of components with which it is securely operably connected;

computer-readable program code means for accessing a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

computer-readable program code means for operating a card reader for accessing the stored secrets and stored identifying information;

computer-readable program code means for detecting and responding to an operable insertion of the card into the card reader; and

computer-readable program code means for securely operably connecting the biometric sensor, the card reader, and the security component.

34. The computer program product according to Claim 33, wherein the stored identifying information comprises stored biometric information of the authorized holder, and further

comprising computer-readable program code means for comparing biometric information obtained with the biometric sensor from a user of the system, to the stored biometric information of the authorized holder.

35. The computer program product according to Claim 33, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

36. The computer program product according to Claim 33, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

37. The computer program product according to Claim 36, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

38. The computer program product according to Claim 33, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

39. The computer program product according to Claim 33, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

40. The computer program product according to Claim 33, wherein the computer-readable program code means for securely operably connecting further comprises computer-readable program code means for authenticating the biometric sensor and the card reader to the security component.

41. The computer program product according to Claim 40, further comprising computer-readable program code means for authenticating the security component to the biometric sensor and the card reader.

42. The computer program product according to Claim 33, wherein the computer-readable program code means for securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

43. The computer program product according to Claim 40, wherein the computer-readable program code means for authenticating the biometric sensor and the card reader are securely stored thereon.

44. The computer program product according to Claim 40, wherein the computer-readable program code means for authenticating further comprises computer-readable program code means for using public key cryptography.

45. The computer program product according to Claim 34, further comprising computer-readable program code means for concluding that the user is the authorized holder of the card only if the means for comparing succeeds.

46. The computer program product according to Claim 33, wherein the card is a smart card.

47. The computer program product according to Claim 34, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising computer-readable program code means for digitally signing information presented to the card with the private key if the computer-readable program code means for comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

48. The computer program product according to Claim 34, wherein the computer-readable program code means for comparing is performed by the biometric sensor.

49. The computer program product according to Claim 48, further comprising computer-readable program code means for securely transferring the stored biometric information of the authorized holder to the biometric sensor for use by the computer-readable program code means for comparing.

50. The computer program product according to Claim 49, further comprising computer-readable program code means for interrupting the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

51. The computer program product according to Claim 34, wherein the computer-readable program code means for comparing is performed by the security component.

52. The computer program product according to Claim 47, further comprising computer-readable program code means for securely operably connecting an application processing component to the security component, and wherein the information presented to the card is generated by the securely operably connected application processing component.

53. The computer program product according to Claim 40, wherein the computer-readable program code means for authenticating further comprises computer-readable program code means for performing a security handshake between the biometric sensor and the security component and between the card reader and the security component.

54. The computer program product according to Claim 53, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

55. The computer program product according to Claim 40, wherein:

the computer-readable program code means for authenticating the biometric sensor further comprises computer-readable program code means for using (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

the computer-readable program code means for authenticating the card reader further comprises computer-readable program code means for using (1) a second unique identifier of the card reader, (2) a second digital signature computed over the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.

56. A method of securely providing biometric input from a user, comprising steps of:

operating a biometric sensor;

operating a security component which provides security functions, such that the security component can vouch for authenticity of components with which it is securely operably connected;

accessing a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

operating a card reader for accessing the stored secrets and stored identifying information;

detecting and responding to an operable insertion of the card into the card reader; and

securely operably connecting the biometric sensor, the card reader, and the security component.

57. The method product according to Claim 56, wherein the stored identifying information comprises stored biometric information of the authorized holder, and further comprising the step of comparing biometric information obtained with the biometric sensor from a user of the system, to the stored biometric information of the authorized holder.

58. The method according to Claim 56, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

59. The method according to Claim 56, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

60. The method according to Claim 59, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

61. The method according to Claim 56, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

62. The method according to Claim 56, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

63. The method according to Claim 56, wherein the step of securely operably connecting further comprises the step of authenticating the biometric sensor and the card reader to the security component.

64. The method according to Claim 63, further comprising the step of authenticating the security component to the biometric sensor and the card reader.

65. The method according to Claim 56, wherein the step of securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

66. The method according to Claim 63, wherein instructions for authenticating the biometric sensor and the card reader are securely stored thereon.

67. The method according to Claim 63, wherein the step of authenticating further comprises the step of using public key cryptography.

68. The method according to Claim 57, further comprising the step of concluding that the user is the authorized holder of the card only if the comparing step succeeds.

69. The method according to Claim 56, wherein the card is a smart card.

70. The method according to Claim 57, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising the step of digitally signing information presented to the card with the private key if the step of comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

71. The method according to Claim 57, wherein the step of comparing is performed by the biometric sensor.

72. The method according to Claim 71, further comprising the step of securely transferring the stored biometric information of the authorized holder to the biometric sensor for use the step of comparing.

73. The method according to Claim 72, further comprising the step of interrupting the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

74. The method according to Claim 57, wherein the step of comparing is performed by the security component.

75. The method according to Claim 70, further comprising the step of securely operably connecting an application processing component to the security component, and wherein the information presented to the card is generated by the securely operably connected application processing component.

76. The method according to Claim 63, wherein the step of authenticating further comprises the step of performing a security handshake between the biometric sensor and the security component and between the card reader and the security component.

77. The method according to Claim 76, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

78. The method according to Claim 63, wherein:

the step of authenticating the biometric sensor further comprises the step of using (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

the step of authenticating the card reader further comprises the step of using (1) a second unique identifier of the card reader, (2) a second digital signature computed over the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.